

Computing automorphic forms on Shimura curves over fields with arbitrary class number

John Voight

Department of Mathematics and Statistics
University of Vermont
16 Colchester Ave
Burlington, VT 05401, USA
jvoight@gmail.com

Abstract. We extend methods of Greenberg and the author to compute in the cohomology of a Shimura curve defined over a totally real field with arbitrary class number. Via the Jacquet-Langlands correspondence, we thereby compute systems of Hecke eigenvalues associated to Hilbert modular forms of arbitrary level over a totally real field of odd degree. We conclude with two examples which illustrate the effectiveness of our algorithms.

The development and implementation of algorithms to compute with automorphic forms has emerged as a major topic in explicit arithmetic geometry. The first such computations were carried out for elliptic modular forms, and now very large and useful databases of such forms exist [2,13,14]. Recently, effective algorithms to compute with Hilbert modular forms over a totally real field F have been advanced. The first such method is due to Dembélé [4,5], who worked initially under the assumption that F has even degree $n = [F : \mathbb{Q}]$ and strict class number 1. Exploiting the Jacquet-Langlands correspondence, systems of Hecke eigenvalues can be identified inside spaces of automorphic forms on B^\times , where B is the quaternion algebra over F ramified precisely at the infinite places of F —whence the assumption that n is even. Dembélé then provides a computationally efficient theory of Brandt matrices associated to B . This method was later extended (in a nontrivial way) to fields F of arbitrary class number by Dembélé and Donnelly [6].

When the degree n is odd, a different algorithm has been proposed by Greenberg and the author [8], again under the assumption that F has strict class number 1. This method instead locates systems of Hecke eigenvalues in the (degree one) cohomology of a Shimura curve, now associated to the quaternion algebra B ramified at all but one real place and no finite place. This method uses in a critical way the computation of a fundamental domain and a reduction theory for the associated quaternionic unit group [16]; see Section 1 for an overview. In this article, we extend this method to the case where F has arbitrary (strict) class number. Our main result is as follows; we refer the reader to Sections 1 and 2 for precise definitions and notation.

Theorem 1. *There exists an (explicit) algorithm which, given a totally real field F of degree $n = [F : \mathbb{Q}]$, a quaternion algebra B over F ramified at all but one real place, an ideal \mathfrak{N} of F coprime to the discriminant \mathfrak{D} of B , and a weight $k \in (2\mathbb{Z}_{>0})^n$, computes the system of eigenvalues for the Hecke operators $T_{\mathfrak{p}}$ with $\mathfrak{p} \nmid \mathfrak{D}\mathfrak{N}$ and the Atkin-Lehner involutions $W_{\mathfrak{p}^e}$ with $\mathfrak{p}^e \parallel \mathfrak{D}\mathfrak{N}$ acting on the space of quaternionic modular forms $S_k^B(\mathfrak{N})$ of weight k and level \mathfrak{N} for B .*

In other words, there exists an explicit finite procedure which takes as input the field F , its ring of integers \mathbb{Z}_F , a quaternion algebra B over F , an ideal $\mathfrak{N} \subset \mathbb{Z}_F$, and the vector k encoded in bits (each in the usual way), and outputs a finite set of number fields $E_f \subset \overline{\mathbb{Q}}$ and sequences $(a_f(\mathfrak{p}))_{\mathfrak{p}}$ encoding the Hecke eigenvalues for each cusp form constituent f in $S_k^B(\mathfrak{N})$, with $a_f(\mathfrak{p}) \in E_f$.

From the Jacquet-Langlands correspondence, applying the above theorem to the special case where $\mathfrak{D} = (1)$ (and hence $n = [F : \mathbb{Q}]$ is odd), we have the following corollary.

Corollary 2. *There exists an algorithm which, given a totally real field F of odd degree $n = [F : \mathbb{Q}]$, an ideal \mathfrak{N} of F , and a weight $k \in (2\mathbb{Z}_{>0})^n$, computes the system of eigenvalues for the Hecke operators $T_{\mathfrak{p}}$ and Atkin-Lehner involutions $W_{\mathfrak{p}^e}$ acting on the space of Hilbert modular cusp forms $S_k(\mathfrak{N})$ of weight k and level \mathfrak{N} .*

This corollary is not stated in its strongest form: in fact, our methods overlap with the methods of Dembél  and his coauthors whenever there is a prime \mathfrak{p} which exactly divides the level; see Remark 5 for more detail. Combining these methods, Donnelly and the author [7] are systematically enumerating tables of Hilbert modular forms, and the details of these computations (including the dependence on the weight, level, and class number, as well as a comparison of the runtime complexity of the steps involved) will be reported there [7], after further careful optimization.

A third technique to compute with automorphic forms, including Hilbert modular forms, has been advanced by Gunnells and Yasaki [9]. They instead use the theory of Vorono  reduction and sharply complexes; their work is independent of either of the above approaches.

This article is organized as follows. In Section 1, we give an overview of the basic algorithm of Greenberg and the author which works over fields F with strict class number 1. In Section 2, using an adelic language we address the complications which arise over fields of arbitrary class number, and in Section 3 we make this theory concrete and provide the explicit algorithms announced in Theorem 1. Finally, in Section 4, we consider two examples, one in detail; our computations are performed in the computer system **Magma** [1].

The author would like to thank Steve Donnelly and Matthew Greenberg for helpful discussions as well as the referees for their comments. The author was supported by NSF Grant No. DMS-0901971.

1 An overview of the algorithm for strict class number 1

In this section, we introduce the basic algorithm of Greenberg and the author [8] with a view to extending its scope to base fields of arbitrary class number; for further reading, see the references contained therein.

Let F be a totally real field of degree $n = [F : \mathbb{Q}]$ with ring of integers \mathbb{Z}_F . Let F_+^\times be the group of totally positive elements of F and let $\mathbb{Z}_{F,+}^\times = \mathbb{Z}_F^\times \cap F_+^\times$. Let B be a quaternion algebra over F of discriminant \mathfrak{D} . Suppose that B is split at a unique real place v_1 , corresponding to an embedding $\iota_\infty : B \hookrightarrow B \otimes \mathbb{R} \cong M_2(\mathbb{R})$, and ramified at the other real places v_2, \dots, v_n . Let $\mathcal{O}(1) \subset B$ be a maximal order and let

$$\mathcal{O}(1)_+^\times = \{\gamma \in \mathcal{O}(1)^\times : v_1(\text{nrd}(\gamma)) > 0\} = \{\gamma \in \mathcal{O}(1) : \text{nrd}(\gamma) \in \mathbb{Z}_{F,+}^\times\}$$

denote the group of units of $\mathcal{O}(1)$ with totally positive reduced norm. Let

$$\Gamma(1) = \iota_\infty(\mathcal{O}(1)_+^\times / \mathbb{Z}_F^\times) \subset \text{PGL}_2(\mathbb{R})^+,$$

so that $\Gamma(1)$ acts on the upper half-plane $\mathcal{H} = \{z \in \mathbb{C} : \text{Im}(z) > 0\}$ by linear fractional transformations. Let $\mathfrak{N} \subset \mathbb{Z}_F$ be an ideal coprime to \mathfrak{D} , let $\mathcal{O} = \mathcal{O}_0(\mathfrak{N})$ be an Eichler order of level \mathfrak{N} , and let $\Gamma = \Gamma_0(\mathfrak{N}) = \iota_\infty(\mathcal{O}_0(\mathfrak{N})_+^\times / \mathbb{Z}_F^\times)$.

Let $k = (k_1, \dots, k_n) \in (2\mathbb{Z}_{>0})^n$ be a weight vector; for example, the case $k = (2, \dots, 2)$ of parallel weight 2 is of significant interest. Let $S_k^B(\mathfrak{N})$ denote the finite-dimensional \mathbb{C} -vector space of quaternionic modular forms of weight k and level \mathfrak{N} for B . Roughly speaking, a form $f \in S_k^B(\mathfrak{N})$ is an analytic function $f : \mathcal{H} \rightarrow W_k(\mathbb{C})$ which is invariant under the weight k action by the group $\gamma \in \Gamma$, where $W_k(\mathbb{C})$ is an explicit right B^\times -module [8, (2.4)] and $W_k(\mathbb{C}) = \mathbb{C}$ when k is parallel weight 2. The space $S_k^B(\mathfrak{N})$ comes equipped with the action of Hecke operators $T_{\mathfrak{p}}$ for primes $\mathfrak{p} \nmid \mathfrak{D}\mathfrak{N}$ and Atkin-Lehner involutions $W_{\mathfrak{p}^e}$ for prime powers $\mathfrak{p}^e \parallel \mathfrak{D}\mathfrak{N}$.

The Jacquet-Langlands correspondence [8, Theorem 2.9] (see Hida [10, Proposition 2.12]) gives an isomorphism of Hecke modules

$$S_k^B(\mathfrak{N}) \xrightarrow{\sim} S_k(\mathfrak{D}\mathfrak{N})^{\mathfrak{D}\text{-new}},$$

where $S_k(\mathfrak{D}\mathfrak{N})^{\mathfrak{D}\text{-new}}$ denotes the space of Hilbert modular cusp forms of weight k and level $\mathfrak{D}\mathfrak{N}$ which are new at all primes dividing \mathfrak{D} . Therefore, as Hecke modules one can compute equivalently with Hilbert cusp forms or with quaternionic modular forms.

We compute with the Hecke module $S_k^B(\mathfrak{N})$ by identifying it as a subspace in the degree one cohomology of $\Gamma(1)$, as follows. Let $V_k(\mathbb{C})$ be the subspace of the algebra $\mathbb{C}[x_1, y_1, \dots, x_n, y_n]$ consisting of those polynomials q which are homogeneous in (x_i, y_i) of degree $w_i = k_i - 2$. Then $V_k(\mathbb{C})$ has a right action of the group B^\times given by

$$q^\gamma(x_1, y_1, \dots, x_n, y_n) = \left(\prod_{i=1}^n (\det \gamma_i)^{-w_i/2} \right) q((x_1 \ y_1) \overline{\gamma}_1, \dots, (x_n \ y_n) \overline{\gamma}_n) \quad (1)$$

for $\gamma \in B^\times$, where $\bar{}$ denotes the standard involution (conjugation) on B and $\gamma_i = v_i(\gamma) \in M_2(\mathbb{C})$. By the theorem of Eichler and Shimura [8, Theorem 3.8], we have an isomorphism of Hecke modules

$$S_k^B(\mathfrak{N}) \xrightarrow{\sim} H^1(\Gamma, V_k(\mathbb{C}))^+$$

where the group cohomology H^1 denotes the (finite-dimensional) \mathbb{C} -vector space of crossed homomorphisms $f : \Gamma \rightarrow V_k(\mathbb{C})$ modulo coboundaries and $+$ denotes the $+1$ -eigenspace for complex conjugation. By Shapiro's lemma [8, §6], we then have a further identification

$$S_k^B(\mathfrak{N}) \xrightarrow{\sim} H^1(\Gamma, V_k(\mathbb{C}))^+ \cong H^1(\Gamma(1), V(\mathbb{C}))^+, \quad (2)$$

where $V(\mathbb{C}) = \text{Coind}_\Gamma^{\Gamma(1)} V_k(\mathbb{C})$.

In the isomorphism (2), the Hecke operators act as follows. Let \mathfrak{p} be a prime of \mathbb{Z}_F with $\mathfrak{p} \nmid \mathfrak{D}\mathfrak{N}$ and let $\mathbb{F}_{\mathfrak{p}}$ denote the residue class field of \mathfrak{p} . Since F has strict class number 1, by strong approximation [15, Théorème III.4.3] there exists $\pi \in \mathcal{O}$ such that $\text{nrd } \pi$ is a totally positive generator for \mathfrak{p} . It follows that there are elements $\gamma_a \in \mathcal{O}_+^\times$, indexed by $a \in \mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})$, such that

$$\mathcal{O}_+^\times \pi \mathcal{O}_+^\times = \bigsqcup_{a \in \mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})} \mathcal{O}_+^\times \alpha_a \quad (3)$$

where $\alpha_a = \pi \gamma_a$.

Let $f : \Gamma(1) \rightarrow V(\mathbb{C})$ be a crossed homomorphism, and let $\gamma \in \Gamma(1)$. The decomposition (3) extends to $\mathcal{O}(1)$ as

$$\mathcal{O}(1)_+^\times \pi \mathcal{O}(1)_+^\times = \bigsqcup_{a \in \mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})} \mathcal{O}(1)_+^\times \alpha_a.$$

Thus, there are elements $\delta_a \in \mathcal{O}(1)_+^\times$ for $a \in \mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})$ and a unique permutation γ^* of $\mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})$ such that

$$\alpha_a \gamma = \delta_a \alpha_{\gamma^* a} \quad (4)$$

for all a . We then define $f|T_{\mathfrak{p}} : \Gamma(1) \rightarrow V(\mathbb{C})$ by

$$(f|T_{\mathfrak{p}})(\gamma) = \sum_{a \in \mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})} f(\delta_a)^{\alpha_a}. \quad (5)$$

The space $S_k^B(\mathfrak{N})$ similarly admits an action of Atkin-Lehner operators $W_{\mathfrak{p}^e}$ for primes $\mathfrak{p}^e \parallel \mathfrak{D}\mathfrak{N}$.

From this description, we see that the Hecke module $H^1(\Gamma(1), V(\mathbb{C}))^+$ is amenable to explicit computation. First, we compute a finite presentation for $\Gamma(1)$ with a minimal set of generators G and a solution to the word problem for the computed presentation using an algorithm of the author [16]. Given such a set of generators and relations, one can explicitly find a basis for the \mathbb{C} -vector space $H^1(\Gamma(1), V(\mathbb{C}))$ [8, §5].

We then compute the action of the Hecke operator $T_{\mathfrak{p}}$ on $H^1(\Gamma(1), V(\mathbb{C}))$. We first compute a splitting $\iota_{\mathfrak{p}} : \mathcal{O} \hookrightarrow M_2(\mathbb{Z}_{F, \mathfrak{p}})$. The elements α_a in (4) are then generators with totally positive reduced norm of the left ideals

$$I_a = \mathcal{O}\iota_{\mathfrak{p}}^{-1} \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} + \mathcal{O}\mathfrak{p} \quad (6)$$

and are obtained by principalizing the ideals I_a ; here again we use strong approximation and the hypothesis that F has strict class number 1. Then for each $a \in \mathbb{P}^1(\mathbb{F}_p)$ and each $\gamma \in G$, we compute the permutation γ^* [8, Algorithm 5.8] and the element $\delta_a = \alpha_a \gamma \alpha_{\gamma^* a}^{-1} \in \Gamma(1)$ as in (4). Using the solution to the word problem, we then write δ_a as a word in the generators G for $\Gamma(1)$, and then for a basis of crossed homomorphisms f we compute $f|T_{\mathfrak{p}}$ by computing $(f|T_{\mathfrak{p}})(\gamma) \in V(\mathbb{C})$ for each $\gamma \in G$ as in (5). In a similar way, we compute the action of complex conjugation and the Atkin-Lehner involutions. We then decompose the space $H^1(\Gamma, V(\mathbb{C}))$ under the action of these operators into Hecke irreducible subspaces, and from this we compute the systems of Hecke eigenvalues using linear algebra.

2 The indefinite method with arbitrary class number

In this section, we show how to extend the method introduced in the previous section to the case where F has arbitrary class number [8, Remark 3.11]. We refer the reader to Hida [11] for further background.

2.1 Setup

We carry over the notation from Section 1. Recall that $\mathcal{O} = \mathcal{O}_0(\mathfrak{N})$ is an Eichler order of level \mathfrak{N} in the maximal order $\mathcal{O}(1) \subset B$.

Let $\mathcal{H}^{\pm} = \{z \in \mathbb{C} : \text{Im}(z) \neq 0\} = \mathbb{C} \setminus \mathbb{R}$ be the union of the upper and lower half-planes. Then via ι_{∞} , the group B^{\times} acts on \mathcal{H}^{\pm} by linear fractional transformations.

In this generality, we find it most elucidating to employ adelic notation. Let $\widehat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z}$ and let $\widehat{\cdot}$ denote tensor with $\widehat{\mathbb{Z}}$ over \mathbb{Z} . Consider the double coset

$$X(\mathbb{C}) = B^{\times} \backslash (\mathcal{H}^{\pm} \times \widehat{B}^{\times} / \widehat{\mathcal{O}}^{\times}),$$

where B^{\times} acts on $\widehat{B}^{\times} / \widehat{\mathcal{O}}^{\times}$ by left multiplication via the diagonal embedding. Then $X(\mathbb{C})$ has the structure of a complex analytic space [3] which fails to be compact if and only if $B \cong M_2(\mathbb{Q})$, corresponding to the classical case of elliptic modular forms—higher class number issues do not arise in this case, so from now we assume that B is a division ring.

We again write $S_k^B(\mathfrak{N})$ for the finite-dimensional \mathbb{C} -vector space of quaternionic modular forms of weight k and level \mathfrak{N} : here, again roughly speaking, a quaternionic modular form of weight $k \in (2\mathbb{Z}_{>0})^n$ and level \mathfrak{N} for B is an analytic function

$$f : \mathcal{H}^{\pm} \times \widehat{B}^{\times} / \widehat{\mathcal{O}}^{\times} \rightarrow W_k(\mathbb{C})$$

which is invariant under the weight k action of B^{\times} , with $W_k(\mathbb{C})$ as in Section 1.

2.2 Decomposing the double coset space

By Eichler's theorem of norms, we have $\text{nrd}(B^\times) = F_{(+)}^\times$ where

$$F_{(+)}^\times = \{a \in F^\times : v_i(a) > 0 \text{ for } i = 2, \dots, n\}$$

is the subgroup of elements of F which are positive at all real places which are ramified in B . In particular, $B^\times/B_+^\times \cong \mathbb{Z}/2\mathbb{Z}$, where

$$B_+^\times = \{\gamma \in B^\times : v_1(\text{nrd}(\gamma)) > 0\} = \{\gamma \in B : \text{nrd}(\gamma) \in F_+^\times\}.$$

The group B_+^\times acts on the upper half-plane \mathcal{H} , therefore we may identify

$$X(\mathbb{C}) = B_+^\times \backslash (\mathcal{H} \times \widehat{B}^\times / \widehat{\mathcal{O}}^\times).$$

Now we have a natural (continuous) projection map

$$X(\mathbb{C}) \rightarrow B_+^\times \backslash \widehat{B}^\times / \widehat{\mathcal{O}}^\times,$$

and by strong approximation [15, Théorème III.4.3] the reduced norm gives a bijection

$$\text{nrd} : B_+^\times \backslash \widehat{B}^\times / \widehat{\mathcal{O}}^\times \xrightarrow{\sim} F_+^\times \backslash \widehat{F}^\times / \widehat{\mathbb{Z}}_F^\times \cong \text{Cl}^+ \mathbb{Z}_F, \quad (7)$$

where $\text{Cl}^+ \mathbb{Z}_F$ denotes the strict class group of \mathbb{Z}_F , i.e. the ray class group of \mathbb{Z}_F with modulus equal to the product of all real (infinite) places of F .

The space $X(\mathbb{C})$ is therefore the disjoint union of Riemann surfaces indexed by $\text{Cl}^+ \mathbb{Z}_F$, which we identify explicitly as follows. Let the ideals $\mathfrak{b} \subset \mathbb{Z}_F$ form a set of representatives for $\text{Cl}^+ \mathbb{Z}_F$, and let $\widehat{b} \in \widehat{\mathbb{Z}}_F^\times$ be such that $\widehat{b} \widehat{\mathbb{Z}}_F \cap \mathbb{Z}_F = \mathfrak{b}$. For expositional simplicity, choose $\mathfrak{b} = \mathbb{Z}_F$ and $\widehat{\beta} = \widehat{1}$ for the representatives of the trivial class. By strong approximation (7), there exists $\widehat{\beta} \in \widehat{B}^\times$ such that $\text{nrd}(\widehat{\beta}) = \widehat{b}$. Therefore

$$X(\mathbb{C}) = \bigsqcup_{[\mathfrak{b}]} B_+^\times (\mathcal{H} \times \widehat{\beta} \widehat{\mathcal{O}}^\times). \quad (8)$$

We have a map

$$\begin{aligned} B_+^\times (\mathcal{H} \times \widehat{\beta} \widehat{\mathcal{O}}^\times) &\rightarrow \mathcal{O}_{\widehat{\beta},+}^\times \backslash \mathcal{H} \\ (z, \widehat{\beta} \widehat{\mathcal{O}}^\times) &\mapsto z \end{aligned}$$

where $\mathcal{O}_{\widehat{\beta}} = \widehat{\beta} \widehat{\mathcal{O}} \widehat{\beta}^{-1} \cap B$ and $\mathcal{O}_{\widehat{\beta},+}^\times = \mathcal{O}_{\widehat{\beta}}^\times \cap B_+^\times$, so that $\mathcal{O}_{\widehat{1}} = \mathcal{O}$.

For each $\widehat{\beta}$, let $\Gamma_{\widehat{\beta}} = \iota_\infty(\mathcal{O}_{\widehat{\beta},+}^\times / \mathbb{Z}_F^\times) \subset \text{PGL}_2(\mathbb{R})^+$. Then the Eichler-Shimura isomorphism on each component in (8) gives an identification of Hecke modules

$$S_k^B(\mathfrak{N}) \xrightarrow{\sim} \bigoplus_{\widehat{\beta}} H^1(\Gamma_{\widehat{\beta}}, V_k(\mathbb{C}))^+, \quad (9)$$

where $^+$ denotes the +1-eigenspace for complex conjugation. For each $\widehat{\beta}$, let $\mathcal{O}(1)_{\widehat{\beta}} = \widehat{\beta} \mathcal{O}(1) \widehat{\beta}^{-1} \cap B$ be the maximal order containing the Eichler order $\mathcal{O}_{\widehat{\beta}}$,

and let $\Gamma(1)_{\hat{\beta}} = \iota_{\infty}(\mathcal{O}(1)_{\hat{\beta},+}^{\times}/\mathbb{Z}_F^{\times})$. Further, let $V_{\hat{\beta}}(\mathbb{C}) = \text{Coind}_{\Gamma_{\hat{\beta}}}^{\Gamma(1)_{\hat{\beta}}} V_k(\mathbb{C})$. Then Shapiro's lemma applied to each summand in (9) gives

$$S_k^B(\mathfrak{N}) \xrightarrow{\sim} \bigoplus_{\hat{\beta}} H^1(\Gamma(1)_{\hat{\beta}}, V_{\hat{\beta}}(\mathbb{C}))^+. \quad (10)$$

2.3 Hecke operators

In the description (10), the Hecke operators $T_{\mathfrak{p}}$ act on $\bigoplus_{\hat{\beta}} H^1(\Gamma(1)_{\hat{\beta}}, V_{\hat{\beta}}(\mathbb{C}))$ in the following way. Let \mathfrak{p} be a prime ideal of \mathbb{Z}_F with $\mathfrak{p} \nmid \mathfrak{D}\mathfrak{N}$, and let $\hat{p} \in \hat{\mathbb{Z}}_F$ be such that $\hat{p}\hat{\mathbb{Z}}_F \cap \mathbb{Z}_F = \mathfrak{p}$. We consider the $\hat{\beta}'$ -summand in (10), corresponding to the ideal class $[\mathfrak{b}']$. Let $f : \Gamma(1)_{\hat{\beta}'} \rightarrow V_{\hat{\beta}'}(\mathbb{C})$ be a crossed homomorphism: we will then obtain a new crossed homomorphism $f|T_{\mathfrak{p}} : \Gamma(1)_{\hat{\beta}} \rightarrow V_{\hat{\beta}}(\mathbb{C})$, where $\hat{\beta}$ corresponds to the ideal class of $[\mathfrak{p}\mathfrak{b}']$ among the explicit choices made above.

Let $\hat{\omega} \in \hat{\mathcal{O}}_{\hat{\beta}}$ be such that $\text{nrd}(\hat{\omega}) = \hat{p}$. Then there are elements $\hat{\gamma}_a \in \hat{\mathcal{O}}_{\hat{\beta}}$, indexed by $a \in \mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})$, such that

$$\hat{\mathcal{O}}_{\hat{\beta}}^{\times} \hat{\omega} \hat{\mathcal{O}}_{\hat{\beta}}^{\times} = \bigsqcup_{a \in \mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})} \hat{\mathcal{O}}_{\hat{\beta}}^{\times} \hat{\alpha}_a \quad (11)$$

where $\hat{\alpha}_a = \hat{\omega} \hat{\gamma}_a$.

Let $\gamma \in \Gamma_{\hat{\beta}}$. Extending (11) to $\hat{\mathcal{O}}(1)_{\hat{\beta}}^{\times}$, we conclude that there exist unique elements $\hat{\delta}_a \in \hat{\mathcal{O}}(1)_{\hat{\beta}}^{\times}$ and a unique permutation γ^* of $\mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})$ such that

$$\hat{\alpha}_a \gamma = \hat{\delta}_a \hat{\alpha}_{\gamma^* a}$$

for $a \in \mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})$. Thus we have

$$(\hat{\beta}' \hat{\beta}^{-1} \hat{\alpha}_a) \gamma = (\hat{\beta}' \hat{\beta}^{-1}) \hat{\delta}_a \hat{\alpha}_{\gamma^* a} = \hat{\delta}'_a (\hat{\beta}' \hat{\beta}^{-1} \hat{\alpha}_{\gamma^* a}).$$

where $\hat{\delta}'_a = (\hat{\beta}' \hat{\beta}^{-1}) \hat{\delta}_a (\hat{\beta}' \hat{\beta}^{-1})^{-1}$.

Recall that $\hat{\beta}' \hat{\mathcal{O}}$ has left order $\hat{\mathcal{O}}_{\hat{\beta}'}$ and similarly $\hat{\mathcal{O}} \hat{\beta}^{-1}$ has right order $\hat{\mathcal{O}}_{\hat{\beta}}$. Therefore, we may consider the left $\hat{\mathcal{O}}_{\hat{\beta}'}$ -ideal

$$\hat{\mathcal{O}}_{\hat{\beta}'} \hat{\beta}' \hat{\mathcal{O}} \hat{\beta}^{-1} \hat{\mathcal{O}}_{\hat{\beta}} \hat{\alpha}_a \quad (12)$$

noting that the left and right orders in each case match up, so the product is compatible. Next, recall that the elements $\hat{\beta}'$, $\hat{\beta}$, $\hat{\omega}$ have reduced norms corresponding to the ideal classes $[\mathfrak{b}']$, $[\mathfrak{p}\mathfrak{b}']$, and $[\mathfrak{p}]$, respectively. Thus the reduced norm of the left ideal (12) has a trivial ideal class. Therefore, by strong approximation (applied now to left ideals of the order $\mathcal{O}_{\hat{\beta}'}$), for each $a \in \mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})$, there exist elements $\pi'_a \in \mathcal{O}_{\hat{\beta}'} \cap B_+^{\times}$ such that

$$\hat{\mathcal{O}}_{\hat{\beta}'} \hat{\beta}' \hat{\mathcal{O}} \hat{\beta}^{-1} \hat{\alpha}_a \cap B = \mathcal{O}_{\hat{\beta}'} \pi'_a.$$

Hence there exists a unique permutation γ^* of $\mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})$ such that

$$\pi'_a \gamma = \delta'_a \pi'_{\gamma^* a}$$

with $\delta_a \in \mathcal{O}_{\hat{\beta}', +}^\times$. The new crossed homomorphism $f|T_{\mathfrak{p}} : \Gamma_{\hat{\beta}} \rightarrow V_{\hat{\beta}}(\mathbb{C})$ is then defined by the formula

$$(f|T_{\mathfrak{p}})(\gamma) = \sum_{a \in \mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})} f(\delta'_a) \pi'_a$$

for $\gamma \in \Gamma_{\hat{\beta}}$.

2.4 Complex conjugation and Atkin-Lehner involutions

We now define an operator W_∞ which acts by complex conjugation. Let $\text{Cl}^{(+)} \mathbb{Z}_F$ denote the ray class group of \mathbb{Z}_F with modulus equal to the real (infinite) places of F which are ramified in B . Then we have a natural map $\text{Cl}^+ \mathbb{Z}_F \rightarrow \text{Cl}^{(+)} \mathbb{Z}_F$; this map is an isomorphism if and only if there exists a unit $u \in \mathbb{Z}_F^\times$ which satisfies $v_1(u) < 0$ and $v_i(u) > 0$ for the other real places v_i ($i = 2, \dots, n$) of F , otherwise the kernel of this map is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Let $[\mathfrak{m}] \in \text{Cl}^+ \mathbb{Z}_F$ generate the kernel of this map.

Let $f : \Gamma(1)_{\hat{\beta}'} \rightarrow V_{\hat{\beta}'}$ be a crossed homomorphism, and let $\hat{\beta}$ correspond to the ideal class $[\mathfrak{b}'\mathfrak{m}^{-1}]$; we will define the complex conjugate crossed homomorphism $(f|W_\infty) : \Gamma(1)_{\hat{\beta}} \rightarrow V_{\hat{\beta}}(\mathbb{C})$. The left $\mathcal{O}_{\hat{\beta}'}$ -ideal $\hat{\mathcal{O}}_{\hat{\beta}'} \hat{\beta}' \hat{\mathcal{O}}_{\hat{\beta}'}^{-1} \cap B$ has reduced norm corresponding to the ideal class $[\mathfrak{m}] \in \text{Cl}^+ \mathbb{Z}_F$, so there exists a generator $\mu' \in \mathcal{O}_{\hat{\beta}'}$ of this ideal such that $v_1(\text{nrd}(\mu')) < 0$ but $v_i(\text{nrd}(\mu')) > 0$ for $i = 2, \dots, n$. Then given $\gamma \in \Gamma(1)_{\hat{\beta}}$, we define

$$(f|W_\infty)(\gamma) = f(\mu' \gamma \mu'^{-1}) \mu'.$$

Finally, we define the Atkin-Lehner involutions $W_{\mathfrak{p}^e}$ for $\mathfrak{p}^e \parallel \mathfrak{D}\mathfrak{N}$. Let \mathfrak{p} correspond to $\hat{p} \in \widehat{\mathbb{Z}}_F$. Then there exists an element $\hat{\pi} \in \mathcal{O}_{\hat{\beta}}$ which generates the unique two-sided ideal of $\mathcal{O}_{\hat{\beta}}$ of reduced norm generated by \hat{p}^e . The element $\hat{\pi}$ normalizes $\mathcal{O}_{\hat{\beta}}$ and $\hat{\pi}^2 \in \mathcal{O}_{\hat{\beta}}^\times \hat{F}^\times$. Let $\hat{\beta}$ correspond to the ideal class $[\mathfrak{p}\hat{\pi}]$. Then as above, by strong approximation there exists an element $\mu' \in \mathcal{O}_{\hat{\beta}'} \cap B_+^\times$ such that $\mathcal{O}_{\hat{\beta}'} \hat{\beta}' \hat{\pi} \cap B = \mathcal{O}_{\hat{\beta}'} \mu'$. Given $f : \Gamma(1)_{\hat{\beta}'} \rightarrow V_{\hat{\beta}'}$, we then define $(f|W_{\mathfrak{p}^e}) : \Gamma(1)_{\hat{\beta}} \rightarrow V_{\hat{\beta}}(\mathbb{C})$ by

$$(f|W_{\mathfrak{p}^e})(\gamma) = f(\mu' \gamma \mu'^{-1}) \mu'$$

for $\gamma \in \Gamma(1)_{\hat{\beta}}$.

3 Algorithmic methods

In this section, we take the adelic description of Section 2 and show how to compute with it explicitly, proving Theorem 1.

Our algorithm takes as input a totally real field F of degree $[F : \mathbb{Q}] = n$, a quaternion algebra B over F split at a unique real place, an ideal $\mathfrak{N} \subset \mathbb{Z}_F$ coprime to the discriminant \mathfrak{D} of B , a vector $k \in (2\mathbb{Z}_{>0})^n$, and a prime $\mathfrak{p} \nmid \mathfrak{D}\mathfrak{N}$, and outputs the matrix of the Hecke operator $T_{\mathfrak{p}}$ acting on the space $H = \bigoplus_{\hat{\beta}} H^1(\Gamma(1)_{\hat{\beta}}, V_{\hat{\beta}}(\mathbb{C}))^+$ (in the notation of Section 2) with respect to some fixed basis which does not depend on \mathfrak{p} . From these matrices, one decomposes the space H into Hecke-irreducible subspaces by the techniques of basic linear algebra.

Our algorithm follows the form given in the overview in Section 1, so we describe our algorithm in steps, with a description of each step along the way.

Step 1 (Compute a splitting field): Let $K \hookrightarrow \mathbb{C}$ be a Galois number field containing F which splits B : for example, we can take the normal closure of any quadratic field contained in B . Since all computations then occur inside $K \subset \mathbb{C}$, we may work then with coefficient modules over K using exact arithmetic. (This step is only necessary if k is not parallel weight 2, for otherwise the action of B^\times factors through $K = \mathbb{Q}$.)

Step 2 (Compute ideal class representatives): Compute a set of representatives $[\mathfrak{b}]$ for the strict class group $\text{Cl}^+ \mathbb{Z}_F$ with each \mathfrak{b} coprime to $\mathfrak{p}\mathfrak{D}\mathfrak{N}$. (See Remark 4 below.)

Compute a maximal order $\mathcal{O}(1) \subset B$. For each representative ideal \mathfrak{b} , compute a right $\mathcal{O}(1)$ -ideal $J_{\mathfrak{b}}$ such that $\text{nrd}(J_{\mathfrak{b}}) = \mathfrak{b}$ and let $\mathcal{O}(1)_{\mathfrak{b}}$ be the left order of $J_{\mathfrak{b}}$. (In the notation of Section 2, the right $\mathcal{O}(1)$ -ideals $J_{\mathfrak{b}}$ represent the elements $\hat{\beta}$, and $\mathcal{O}(1)_{\mathfrak{b}} = \mathcal{O}(1)_{\hat{\beta}}$.)

Step 3 (Compute presentations for the unit groups): Compute an embedding $\iota_{\infty} : B \hookrightarrow \text{M}_2(\mathbb{R})$ corresponding to the unique split real place.

For each \mathfrak{b} , compute a finite presentation for $\Gamma(1)_{\mathfrak{b}} = \iota_{\infty}(\mathcal{O}(1)_{\mathfrak{b},+}^{\times} / \mathbb{Z}_F^{\times})$ consisting of a (minimal) set of generators $G_{\mathfrak{b}}$ and relations $R_{\mathfrak{b}}$ together with a solution to the word problem for the computed presentation [16]. (Note that the algorithm stated therein [16, Theorem 3.2] is easily extended from units of reduced norm 1 to totally positive units.)

For efficiency, we start by computing such a presentation with generators G associated to the order $\mathcal{O}(1)$ and then for each order $\mathcal{O}(1)_{\mathfrak{b}}$ we begin with the elements in hand formed by short products of elements in G which happen to lie in $\mathcal{O}(1)_{\mathfrak{b}}$ (to aid in the search for units [16, Algorithm 3.2]; note that $\mathcal{O}(1) \cap \mathcal{O}(1)_{\mathfrak{b}}$ is an Eichler order of level \mathfrak{b} in $\mathcal{O}(1)_{\mathfrak{b}}$).

Step 4 (Compute splitting data): Compute a splitting

$$\iota_{\mathfrak{N}} : \mathcal{O}(1) \hookrightarrow \mathcal{O}(1) \otimes_{\mathbb{Z}_F} \mathbb{Z}_{F,\mathfrak{N}} \cong \text{M}_2(\mathbb{Z}_{F,\mathfrak{N}}).$$

Note that since \mathfrak{b} is coprime to \mathfrak{N} , we have $\mathcal{O}(1) \otimes_{\mathbb{Z}_F} \mathbb{Z}_{F,\mathfrak{N}} = \mathcal{O}(1)_{\mathfrak{b}} \otimes_{\mathbb{Z}_F} \mathbb{Z}_{F,\mathfrak{N}}$ for all \mathfrak{b} , so $\iota_{\mathfrak{N}}$ also gives rise to a splitting for each $\mathcal{O}(1)_{\mathfrak{b}}$. For each \mathfrak{b} , compute the Eichler order $\mathcal{O}_{\mathfrak{b}} \subset \mathcal{O}(1)_{\mathfrak{b}}$ of level \mathfrak{N} with respect to $\iota_{\mathfrak{N}}$.

Next, for each \mathfrak{b} , compute representatives for the left cosets of the group $\Gamma_{\mathfrak{b}} = \iota_{\infty}(\mathcal{O}_{\mathfrak{b},+}^{\times} / \mathbb{Z}_F^{\times})$ inside $\Gamma(1)_{\mathfrak{b}}$ [8, Algorithm 6.1]. Finally, identify

$$V(K)_{\mathfrak{b}} = \text{Coind}_{\Gamma_{\mathfrak{b}}}^{\Gamma(1)_{\mathfrak{b}}} V_k(K)$$

as a K -vector space given by copies of $V_k(K)$ indexed by these cosets, and compute the permutation action of the representatives of these cosets on this space.

In practice, it is more efficient to identify the above coset representatives with elements of $\mathbb{P}^1(\mathbb{Z}_F/\mathfrak{N})$ and thereby work directly with the coefficient module $V(K)_\mathfrak{b} \cong K[\mathbb{P}^1(\mathbb{Z}_F/\mathfrak{N})] \otimes V_k(K)$.

Step 5 (Compute a basis for cohomology): Identify the space of crossed homomorphisms $\bigoplus_\mathfrak{b} Z^1(\Gamma(1)_\mathfrak{b}, V(K)_\mathfrak{b})$ with its image under the inclusion

$$\begin{aligned} Z^1(\Gamma_\mathfrak{b}, V(K)_\mathfrak{b}) &\rightarrow \bigoplus_{g \in G_\mathfrak{b}} V(K)_\mathfrak{b} \\ f &\mapsto (f(g))_{g \in G_\mathfrak{b}} \end{aligned}$$

consisting of those $f \in \bigoplus_{g \in G_\mathfrak{b}} V(K)_\mathfrak{b}$ which satisfy the relations $f(r) = 0$ for $r \in R_\mathfrak{b}$. Compute the space of principal crossed homomorphisms $B^1(\Gamma(1)_\mathfrak{b}, V(K)_\mathfrak{b})$ in a similar way, and thereby compute using linear algebra a K -basis for the quotient $H^1(\Gamma(1)_\mathfrak{b}, V(K)_\mathfrak{b}) = Z^1(\Gamma(1)_\mathfrak{b}, V(K)_\mathfrak{b})/B^1(\Gamma(1)_\mathfrak{b}, V(K)_\mathfrak{b})$ for each \mathfrak{b} .

Let $H = \bigoplus_\mathfrak{b} H^1(\Gamma(1)_\mathfrak{b}, V(K)_\mathfrak{b})$.

Step 6 (Compute representatives for left ideal classes): Compute a splitting $\iota_\mathfrak{p} : \mathcal{O}(1) \hookrightarrow M_2(\mathbb{Z}_{F,\mathfrak{p}})$. For each ideal \mathfrak{b}' , perform the following steps.

First, compute the ideal \mathfrak{b} with ideal class $[\mathfrak{b}] = [\mathfrak{p}\mathfrak{b}']$. Compute the left ideals

$$I_a = \mathcal{O}_{\iota_\mathfrak{p}^{-1}} \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} + \mathcal{O}\mathfrak{p}$$

indexed by the elements $a = (x : y) \in \mathbb{P}^1(\mathbb{F}_\mathfrak{p})$ and then compute the left $\mathcal{O}_{\mathfrak{b}'}$ -ideals $I'_a = J_{\mathfrak{b}'} \overline{J}_\mathfrak{b} I_a$.

Compute totally positive generators $\pi'_a \in \mathcal{O}_{\mathfrak{b}'} \cap B_+^\times$ for $\mathcal{O}_{\mathfrak{b}'} \pi'_a = I'_a$ [12].

Now, for each $\gamma \in G_\mathfrak{b}$, compute the permutation γ^* of $\mathbb{P}^1(\mathbb{F}_\mathfrak{p})$ [8, Algorithm 5.8] and then the elements $\delta'_a = \pi'_a \gamma \pi_{\gamma^* a}^{-1}$ for $a \in \mathbb{P}^1(\mathbb{F}_\mathfrak{p})$; write each such element δ'_a as a word in $G'_\mathfrak{b}$ and from the formula

$$(f | T_\mathfrak{p})(\gamma) = \sum_{a \in \mathbb{P}^1(\mathbb{F}_\mathfrak{p})} f(\delta'_a)^{\pi'_a}$$

with f in a basis for the \mathfrak{b}' -component of cohomology as in Step 5 compute the induced crossed homomorphism $f | T_\mathfrak{p}$ in the \mathfrak{b} -component.

Step 7 (Compute the blocks of the intermediate matrix): Assemble the matrix T with rows and columns indexed as in Step 5 with blocks in the $(\mathfrak{b}, \mathfrak{b}')$ position given by the output of Step 6: this matrix describes the action of $T_\mathfrak{p}$ on H .

Step 8 (Decompose H into \pm -eigenspaces for complex conjugation): Determine the representative ideal \mathfrak{m} (among the ideals \mathfrak{b}) which generates the kernel of the map $\text{Cl}^+ \mathbb{Z}_F \rightarrow \text{Cl}^{(+)} \mathbb{Z}_F$.

For each ideal \mathfrak{b}' , perform the following steps. Compute the ideal \mathfrak{b} such that $[\mathfrak{b}] = [\mathfrak{b}'\mathfrak{m}^{-1}]$, and compute a generator μ' with $\mathcal{O}_{\mathfrak{b}'}\mu' = J_{\mathfrak{b}'}\overline{J}_{\mathfrak{b}}$ such that $v(\text{nrd}(\mu')) < 0$. For each $\gamma \in G_{\mathfrak{b}}$, from the formula

$$(f | W_{\infty})(\gamma) = f(\mu'\gamma\mu'^{-1})^{\mu'},$$

for f in a basis for the \mathfrak{b}' -component of cohomology as in Step 5 compute the induced crossed homomorphism $f | T_{\mathfrak{p}}$ in the \mathfrak{b} -component.

Assemble the matrix with blocks in the $(\mathfrak{b}, \mathfrak{b}')$ position given by this output: this matrix describes the action of complex conjugation W_{∞} on H . Compute a K -basis for the $+1$ -eigenspace H^+ of H for W_{∞} . Finally, compute the matrix T^+ giving the action of $T_{\mathfrak{p}}$ restricted to H^+ and return T^+ .

This completes the description of the algorithm.

In a similar way, one computes the Atkin-Lehner involutions, replacing Step 6 with the description given in Section 2.4, similar to the computation of complex conjugation in Step 8.

Remark 3. Note that Steps 1 through 3 do not depend on the prime \mathfrak{p} nor the level \mathfrak{N} and Steps 4, 5, and 8 do not depend on the prime \mathfrak{p} , so these may be precomputed for use in tabulation.

Remark 4. To arrange uniformly that the ideals \mathfrak{b} representing the classes in $\text{Cl}^+ \mathbb{Z}_F$ are coprime to the prime \mathfrak{p} in advance for many primes \mathfrak{p} , one has several options. One possibility is to choose suitable ideals \mathfrak{b} of large norm in advance. Another option is to make suitable modifications “on the fly”: if \mathfrak{p} is not coprime to \mathfrak{b} , we simply choose a different ideal \mathfrak{c} coprime to \mathfrak{p} with $[\mathfrak{b}] = [\mathfrak{c}]$, a new ideal $J_{\mathfrak{c}}$ with $\text{nrd}(J_{\mathfrak{c}}) = \mathfrak{c}$, and compute an element $\nu \in \mathcal{O}_{\mathfrak{b}}$ such that $\nu\mathcal{O}_{\mathfrak{b}}\nu^{-1} = \mathcal{O}_{\mathfrak{c}}$. Conjugating by ν where necessary, one can then transport the computations from one order to the other so no additional computations need to take place.

4 Examples

In this section, we compute with two examples to demonstrate the algorithm outlined in Section 3. Throughout, we use the computer system **Magma** [1].

Our first and most detailed example is concerned with the smallest totally real cubic field F with the property that the dimension of the space of Hilbert cusp forms of parallel weight 2 and level (1) is greater than zero and the strict class number of F is equal to 2. This field is given by $F = \mathbb{Q}(w)$ where w satisfies the equation $f(w) = w^3 - 11w - 11 = 0$. The discriminant of F is equal to $2057 = 11^2 17$, and $\mathbb{Z}_F = \mathbb{Z}[w]$. The roots of f in \mathbb{R} are $-2.602\dots$, $-1.131\dots$, and $3.73\dots$, and we label the real places v_1, v_2, v_3 of F into \mathbb{R} according to this ordering.

We define the *sign* of $a \in F$ to be the triple $\text{sgn}(a) = (\text{sgn}(v_i(a)))_{i=1}^3 \in \{\pm 1\}^3$. The unit group of F is generated by the elements -1 , $w + 1$ with $\text{sgn}(w + 1) = (1, -1, -1)$, and the totally positive unit $-w^2 + 2w + 12$.

We begin by finding a quaternion algebra B with $\mathfrak{D} = \mathbb{Z}_F$ which is ramified at all but one real place [8, Algorithm 4.1]. We find the algebra $B = \left(\frac{w+1, -1}{F} \right)$ ramified only at v_1 and v_2 , generated by i, j subject to $i^2 = w+1$, $j^2 = -1$, and $ji = -ij$.

For forms of parallel weight 2, **Step 1** is trivial: we can take $K = \mathbb{Q}$.

Next, in **Step 2** we compute ideal class representatives. The nontrivial class in $\text{Cl}^+(\mathbb{Z}_F)$ is represented by the ideal $\mathfrak{b} = (w^2 - 2w - 6)\mathbb{Z}_F$, which is principal but does not possess a totally positive generator, since $\text{sgn}(-w^2 + 2w + 6) = (-1, 1, -1)$ and there is no unit of \mathbb{Z}_F with this sign. We note that $N(\mathfrak{b}) = 7$.

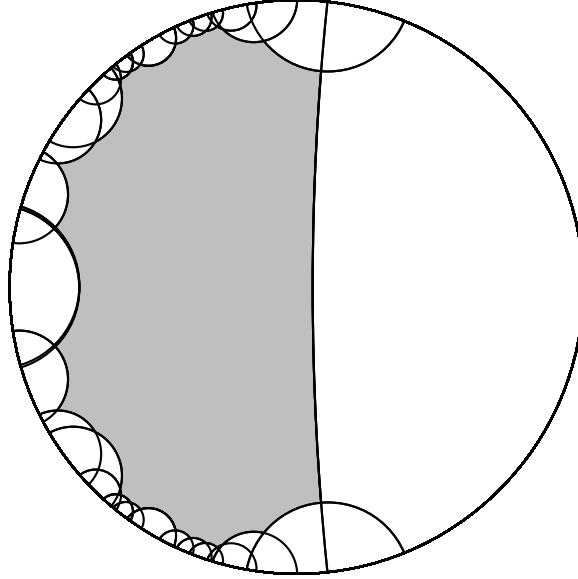
Next, we compute a maximal order $\mathcal{O} = \mathcal{O}(1)$; it is generated over \mathbb{Z}_F by i and the element $k = (1 + (w^2 + 1)i + ij)/2$. Next, we find that the right \mathcal{O} -ideal $J_{\mathfrak{b}}$ generated by $w^2 - 2w - 6$ and the element $(5 + (w^2 + 5)i + ij)/2 = 2 + 2i + k$ has $\text{nr}(J_{\mathfrak{b}}) = \mathfrak{b}$.

Next, in **Step 3** we compute presentations for the unit groups. We take the splitting

$$B \hookrightarrow M_2(\mathbb{R})$$

$$i, j \mapsto \begin{pmatrix} s & 0 \\ 0 & -s \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

where $s = \sqrt{v_3(w+1)}$. We then compute a fundamental domain for $\Gamma = \Gamma(1)$ [16], given below.



We find that $\Gamma = \Gamma(1)$ is the free group on the generators $\alpha, \beta, \gamma_1, \dots, \gamma_7$ subject to the relations

$$\gamma_1^2 = \gamma_2^2 = \gamma_3^3 = \gamma_4^2 = \gamma_5^3 = \gamma_6^2 = \gamma_7^2 = \alpha\beta\alpha^{-1}\beta^{-1}\gamma_1 \cdots \gamma_7 = 1.$$

For example, we have

$$2\alpha = (w^2 - 14) + (2w^2 - 4w - 13)i + (-2w^2 + 5w + 9)j + (-4w^2 + 8w + 26)ij.$$

The groups Γ and $\Gamma_{\mathfrak{b}}$ have isomorphic presentations. In particular, we note that both Γ and $\Gamma_{\mathfrak{b}}$ have genus 1, so we conclude that $\dim S_2(1) = 1 + 1 = 2$.

We illustrate the computation of Hecke operators with the primes $\mathfrak{p}_3 = (w + 2)\mathbb{Z}_F$ of norm 3 and $\mathfrak{p}_5 = (w + 3)\mathbb{Z}_F$ of norm 5. Note that \mathfrak{p}_3 is nontrivial in $\text{Cl}^+(\mathbb{Z}_F)$ whereas \mathfrak{p}_5 is trivial.

Step **Step 4** requires no work, since we work with forms of level (1). In **Step 5** we compute with a basis for cohomology, and here we see directly that

$$H^1(\Gamma, \mathbb{Q}) \cong \text{Hom}(\Gamma, \mathbb{Q}) \cong \mathbb{Z}f_{\alpha} \oplus \mathbb{Z}f_{\beta}$$

where f_{α}, f_{β} are the characteristic functions for α and β . We have a similar description for $H^1(\Gamma_{\mathfrak{b}}, \mathbb{Q})$.

Next, in **Step 6** we compute representatives of the left ideal classes. For \mathfrak{p}_3 , for example, for $I_{[1:0]} \subset \mathcal{O}$ we find that $J_{\mathfrak{b}}I_{[1:0]} = \mathcal{O}_{\mathfrak{b}}((w + 1) + i + ij)$ and for $I_{[1:1]} \subset \mathcal{O}_{\mathfrak{b}}$ we have $\overline{J_{\mathfrak{b}}}I_{[1:1]} = \mathcal{O}(w + 1 - i + ij)$; we thereby find elements π_a, π'_a for $a \in \mathbb{P}^1(\mathbb{F}_{\mathfrak{p}_3})$. For the generators $\gamma = \alpha, \beta$ of \mathcal{O} and $\mathcal{O}_{\mathfrak{b}}$, we compute the permutations γ^* of $\mathbb{P}^1(\mathbb{F}_{\mathfrak{p}_3})$; we find for example that α^* is the identity and

$$\pi'_{[1:0]}\alpha = \delta'_{[1:0]}\pi'_{[1:0]}$$

with $\delta'_{[1:0]} \in \mathcal{O}_{\mathfrak{b}}$, namely,

$$\begin{aligned} 14\delta'_{[1:0]} &= (7w^2 - 98) + (-23w^2 + 40w + 167)i + \\ &\quad (-25w^2 + 59w + 103)j + (-2w^2 + 5w + 20)ij. \end{aligned}$$

We then write $\delta'_{[1:0]}$ as a word in the generators for $\Gamma'_{\mathfrak{b}}$ of length 23. Repeating these steps (reducing a total of 64 units), we assemble the block matrix in **Step 7** as the matrix

$$T_{\mathfrak{p}_3} | H = \begin{pmatrix} 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \\ 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \end{pmatrix}.$$

In a similar way, we find that $T_{\mathfrak{p}_5}$ is the identity matrix.

Finally, in **Step 8** we compute the action of complex conjugation. Here we have simply $\mu = i$ (whereas $\mu_{\mathfrak{b}}$ is more complicated), and thereby compute that

$$W_{\infty} | H = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

We verify that W_{∞} commutes with $T_{\mathfrak{p}_3}$ (and $T_{\mathfrak{p}_5}$). We conclude that $T_{\mathfrak{p}_3} | H^+ = \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}$ and $T_{\mathfrak{p}_5} | H^+ = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

We then diagonalize the space H^+ , which breaks up into two one-dimensional eigenforms f and g , and compute several more Hecke operators: we list in Table 1 below a generator for the prime \mathfrak{p} , its norm $N\mathfrak{p}$, and the Hecke eigenvalues $a_{\mathfrak{p}}(f)$ and $a_{\mathfrak{p}}(g)$ for the cusp forms f, g .

\mathfrak{p}	$N\mathfrak{p}$	$a_{\mathfrak{p}}(f)$	$a_{\mathfrak{p}}(g)$
$w + 2$	3	2	-2
$w + 3$	5	1	1
2	8	-5	-5
$2w + 7$	9	-2	2
w	11	0	0
$w^2 - w - 8$	17	-5	5
$w - 3$	17	-5	-5
$2w^2 - 5w - 10$	23	2	-2
$w^2 - 3w - 2$	25	-9	-9
$w^2 - 6$	29	9	-9
$w + 4$	31	-2	-2
$2w^2 - 3w - 16$	37	-3	3
$w^2 - 2w - 9$	41	-5	5
$w^2 + w - 3$	49	-10	10

Table 1: Hecke eigenvalues for the Hilbert cusp forms for $F = \mathbb{Q}(w)$ with $w^3 - 11w - 11 = 0$ of level (1) and parallel weight 2

We note that the primes generated by w and $w - 3$ are ramified in F .

By work of Deligne [3], the curves $X = X(1)$ and $X_{\mathfrak{b}}$ are defined over the strict class field F^+ of F , and $\text{Gal}(F^+/F)$ permutes them. We compute that $F^+ = F(\sqrt{-3w^2 + 8w + 12})$. Therefore the Jacobian J_f , corresponding to the cusp form f , is a modular elliptic curve over F^+ with $\#J(\mathbb{F}_{\mathfrak{p}}) = N\mathfrak{p} + 1 - a_f(\mathfrak{p})$ with everywhere good reduction. The form g is visibly a quadratic twist of f by the character corresponding to the extension F^+/F .

Unfortunately, this curve does not have any apparent natural torsion structure which would easily allow for its identification as an explicit curve given by a sequence of coefficients [6, §4].

As a second and final example, we compute with a quaternion algebra defined over a quadratic field and therefore ramified at a finite prime. We take $F = \mathbb{Q}(\sqrt{65})$, with $\mathbb{Z}_F = \mathbb{Z}[(1 + \sqrt{65})/2]$. The field F has $\#\text{Cl}(F) = \#\text{Cl}^+(F) = 2$. We compute the space $S = S_2(\mathfrak{p}_5)^{\mathfrak{p}_5\text{-new}}$ of Hilbert cuspidal new forms of parallel weight 2 and level \mathfrak{p}_5 , where \mathfrak{p}_5 is the unique prime in \mathbb{Z}_F of norm 5.

We compute that $\dim S = 10$, and that the space S decomposes into Hecke-irreducible subspaces of dimensions 2, 2, 3, 3. For example, the characteristic polynomial of $T_{\mathfrak{p}_2}$ for \mathfrak{p}_2 either prime above 2 factors as

$$(T^2 - 2T - 1)(T^2 + 2T - 1)(T^6 + 11T^4 + 31T^2 + 9).$$

Remark 5. By the Jacquet-Langlands correspondence, the space $S_2(\mathfrak{p}_5)^{\mathfrak{p}_5\text{-new}}$ also occurs in the space of quaternionic modular forms for an Eichler order of

level \mathfrak{p}_5 in the definite quaternion algebra ramified at the the two real places of F and no finite place, and therefore is amenable to calculation by the work of Dembélé and Donnelly. We use this overlap to duplicate their computations (as well as ours) and thereby give some compelling evidence that the results are correct since they are computed in entirely different ways.

References

1. Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3–4, 235–265.
2. John Cremona, *The elliptic curve database for conductors to 130000*, Algorithmic number theory (Berlin, 2006), Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, 11–29.
3. P. Deligne, *Travaux de Shimura*, Séminaire Bourbaki, Lecture notes in Math. **244**, no. 389, 123–165.
4. Lassina Dembélé, *Explicit computations of Hilbert modular forms on $\mathbb{Q}(\sqrt{5})$* , Experiment. Math. **14** (2005), no. 4, 457–466.
5. L. Dembélé, *Quaternionic Manin symbols, Brandt matrices and Hilbert modular forms*, Math. Comp. **76** (2007), no. 258, 1039–1057.
6. L. Dembélé and S. Donnelly, *Computing Hilbert modular forms over fields with nontrivial class group*, Algorithmic number theory (Banff, 2008), Lecture Notes in Comput. Sci., vol. 5011, Springer, Berlin, 2008, 371–386.
7. Steve Donnelly and John Voight, *Tables of Hilbert modular forms and elliptic curves over totally real fields*, in preparation.
8. Matthew Greenberg and John Voight, *Computing systems of Hecke eigenvalues associated to Hilbert modular forms*, accepted to Math. Comp.
9. Paul Gunnells and Dan Yasaki, *Hecke operators and Hilbert modular forms*, Algorithmic number theory (Berlin, 2008), Lecture Notes in Comput. Sci., vol. 5011, Springer, Berlin, 2008, 387–401.
10. H. Hida, *On abelian varieties with complex multiplication as factors of the Jacobians of Shimura curves*, American Journal of Mathematics **103** no. 4 (1981), 727–776.
11. Haruzo Hida, *Hilbert modular forms and Iwasawa theory*, Clarendon Press, Oxford, 2006.
12. Markus Kirschmer and John Voight, *Algorithmic enumeration of ideal classes for quaternion orders*, SIAM J. Comput. (SICOMP) **39** (2010), no. 5, 1714–1747.
13. William Stein, *Modular forms database*, <http://modular.math.washington.edu/Tables>, 2004.
14. W. A. Stein and M. Watkins, *A database of elliptic curves—first report*, Algorithmic number theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, 267–275.
15. Marie-France Vignéras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Math., vol. 800, Springer, Berlin, 1980.
16. John Voight, *Computing fundamental domains for cofinite Fuchsian groups*, J. Théorie Nombres Bordeaux **21** (2009), no. 2, 467–489.